The Blueprint to Security

As the Internet exploded in popularity and use in the mid-1990s, many private infrastructure companies responsible for providing the public services like electric power, clean water and reliable telecommunication services followed business trends and brought their computer-based control systems online. With a virtual network, employees inside the firewall could instantly access data or trending information, or make operational decisions from control rooms located miles away. The movement toward automated online control helped reduce manpower, increase time and efficiency and cut consumer costs. At the time, the concept of cyber security was in its infancy.

Photo: Tebbe and Gorski

INL engineers Jeff Tebbe and Ed Gorski developed an innovative software program to assist infrastructure owners in applying cyber security standards to their networks.

Today, most companies--having battled a barrage of malicious viruses, worms and outside intrusions--agree that cyber security is a fundamental element to a successful business. Yet even with a strong desire for security, the idea of cyber security standards for private infrastructure company control systems has been a well-debated and divisive concept in the industry. From recommended requirements by the Instrumentation, Systems, and Automation Society (ISA) to the National Institute of Standards and Technology (NIST), an infrastructure company has the option of following dozens of unique, voluntary cyber standards. In fact, a simple Google search on control systems standards results in more than 200 million Web sites, articles and documents on the topic.

Implementing reconfigured firewalls, encryption or authentication while meeting the requirements to provide real-time power, water or gas services to millions of customers can be extremely challenging. Unlike most businesses, utilities must operate continuously, leaving no defined time when control systems can be shut down for software upgrades or security enhancements.

But recently, a team of control system and cyber security researchers from Idaho National Laboratory--working for the Department of Homeland Security's Control Systems Security Program--has developed a new software-based tool that may help settle this debate.

How it Works

The Control System Cyber Security Self-Assessment Tool (CS2SAT) works by compiling many known cyber security standards into one database and provides instructions to companies on how to best meet minimum cyber security recommendations based on their risk of a cyber intrusion. The tool is intended to help establish unified, consistent guidelines that will provide infrastructure control systems with a constant method for gauging and improving their cyber security process, while still allowing utility companies to maximize their productivity over the Internet.

Photo: Tebbe and Gorski

The Control Systems Cyber Security Self Assessment Tool uses a question and answer format to recommend enhanced cyber security techniques and guidelines.

"Every business, product or service follows some kind of industry standard," said INL engineer and tool co-developer Jeff Tebbe. "But with cyber security being such a new and constantly evolving field, there really hasn't been one set of standards that can adequately meet all the unique protocols and security challenges, and still provide the services that are needed by the public."

According to Tebbe, this ambiguity has meant that most control systems manufacturers and owners have applied a wide assortment of cyber standards and personnel security products to their systems without thorough knowledge of their effectiveness. To resolve this issue, the INL team developed an interview-based assessment tool that asks users to supply information about their control system at several steps. The tool then evaluates the answers and provides recommendations for improvement.

The entire process runs on a laptop or desktop computer in about eight hours. Once the tool is loaded, users input data about their control system at four different, but interrelated steps. The first step identifies potential cyber consequences related to the facility being assessed, while the other three provide information and recommendations on how to fix potential weaknesses.

The first step, *Consequence Analysis* , asks users to answer a series of multiple-choice questions related to the potential economic impact, loss of life or injury, environmental and cascading effects of a successful cyber intrusion. Most utilities employ a security analyst who can accurately predict both the physical and financial impacts of such an intrusion. Once the questions have been answered, the tool calculates a recommended Security Assurance Level (SAL) that provides a security goal for utilities to strive for based on their risk associated with a cyber intrusion. The scores range from five, high security, to one, low security. The SAL score is also used to determine which set of existing standards and guidelines located in the tool's database will help guide the company to achieve an appropriate level of security.

For instance, to meet an SAL score of three, typical of most electric power plants, the user's control system would need a minimum of a properly configured firewall placed between the corporate local area network (LAN), and the control system LAN. It would also need encrypted data flow between the corporate and control system network. Control systems not configured for these requirements would be provided a series of recommended steps to help increase their security to an appropriate assurance level.

The second phase is known as *Architecture Discovery* . In this phase, the tool allows users to input data about how their network is configured, and what components such as firewalls, WiFi access points or routers may be connected to the control system. Users also have the option of selecting from standard network configurations, or templates built into the tool. Using a graphical user interface, the tool generates a second series of questions to identify how security has been implemented at each connected component.

According to tool co-developer Ed Gorski, the discovery phase supports identification of each interconnected component even if there aren't any known vulnerabilities.

"By identifying each connected component, users can be proactive in strengthening their security before a major vulnerability or virus hits the Internet," said Gorski. "It helps control system users understand and identify that individual unsecured components can be a gateway into their entire network."

Once the tool identifies all connected components, step three generates a *Requirements Questionnaire* which asks control system engineers and operators to supply specific information about how each control system is currently configured for cyber security. This information is then compared to the SAL score that was assigned to the control system based on its consequence of a cyber intrusion. At this point, the tool generates a gap analysis that identifies which requirements are not being met and recommends a process for improvement.

"Most standards just tell you what requirements you have to meet," said Tebbe. "This tool identifies what industry you belong to, identifies vulnerabilities present in your system and then tells you what cyber standards and techniques you should use to be the most secure."

In addition to security solutions, the final step of the tool displays a *Risk Reduction Report* that prioritizes recommended solutions to ensure increased cyber security is applied to the critical areas first, second and third.

Field Testing

According to Tebbe, industry interest in the CS2SAT tool has been strong because it allows companies to apply security standards based on factual data.

"We didn't want to build a tool that only suggested additional security requirements without allowing industry to be part of process," said Tebbe. "With this tool, users provide data about their system, and the tool tells them how to increase their security based on known and vetted standards."

The Control Systems Security Program has completed initial field testing with seven companies in multiple sectors including water and energy. Additionally, the tool has been demonstrated and discussed at control systems user groups and at conferences like the DHS Process Control Systems Forum. In the near future, researchers hope to commercialize, or hand over, the tool to standards bodies who will oversee distribution to private industry.

General Contact:
Ethan Huffman, (208) 526-0660,

Feature Archive